Data Security in the Modern Age: An Application and Implementation of Data Encryption and Decryption

Wasiu Opeyemi Oduola, Ekele Asonye, Emmanuel Okereke
Department of Electrical and Computer Engineering,
Prairie View A& M University, Texas A & M University System, Texas, USA.
[woduola, easonye, eokereke]@student.pvamu.edu

Victoria A. Bamgbose
Department of Nutritionand Dietetics, Federal University of Agriculture, Abeokuta, Nigeria.
vikkyprogressive@yahoo.com

Abstract
The explosive growth of data in the Internet and digital age and the exponential demands for mobile devices, smart devices, wireless and wired sensors, social networks, personalized healthcare and other data-centric technologies has permeated through every facets of our personal, educational, professional, corporate and government lives. The ubiquity of data has resulted into an increasing number of data breaches and security vulnerabilities in data storage worldwide. Thus, there is a heightened effort globally to strengthen the security of data storage and data sharing to protect mankind against the malicious adversaries intending to tamper with thedata, pose a threat to the freedom of information and individual and collective privacy.This study therefore focuses on the design and implementation of a data decryption and encryption algorithmic module using the field programmable gate array (FPGA) NEXYS 2 board and Xilinx Integrated Synthesis Environment (ISE) 14.6 development tool kit. The design is applicable in instances where two or more parties exchange private and confidential information by helping to eliminate the possibility of eavesdropping or attack from a malicious adversary.

Keywords: *Data security, privacy, encryption, decryption, cryptography, education.*

Introduction

Data security refers to the integrity, availability and confidentiality of data. It entails all the processes and practices involved in ensuring that the data is not accessible or being explored by an unauthorized party or individual. It guarantees the accuracy, reliability and the availability of the data whenever the authorized users need to access the data or extract relevant knowledge and make predictions or trends from the data [1]. But, the ubiquity of data and its intensive usage for several applications has made data security, privacy and trustworthiness an ever-present critical requirement.

The exponential growth of data in the Internet age and the explosive demands for mobile devices, smart devices, wireless and wired sensors, social networks and personalized healthcare has permeated through several facets of human's personal, educational, professional, corporate and government lives [1]. The advent of the Internet of things(IoT) and the widespread data gathering from many smart devices further complicates the challenges concerning data usage, security and the definition of public and private data. This is very concerning considering the fact that over 90% of the global data has been generated within the last ten years alone. Data security and protection of privacy will be more critical in the next few years as digitization of each facet of our daily lives continue to expand [1-5].

Due to the increasing number of data breaches and security vulnerabilities in data storage, there is a heightened effort globally to strengthen the security of data storage and data sharing[2] making it very difficult for the cyber-hackers to tamper with data and pose a threat to the freedom of information. The migration to the cloud as a platform for data storage, retrieval and processing creates another layer in the existing and complex data ecosystems. Malicious hackers can imperil cloud applications and cloud systems gaining access to private data and tamper or delete the data in order to erode users' trust in the data.

To ensure the safety and security of our communities, citizens and nations and for the access to information to improve each aspect of human lives, the relevant data must be secured and protected. There are extensive and active research studies regarding the design of techniques for data security such as the encryption algorithms that support privacy-protecting search over encrypted information [6] as well as algorithms for assessing the trustworthiness of data and the integrity of complex data [7]. But in spite of such high number of data preservation studies, the challenge of data security and protection in the Internet of things and big data age is very problematic. Hence there is the need to design efficient algorithms to ensure the confidentiality of data storage in the cloud. It is crucial to note that the developed algorithms should be aligned with the particular data usage. Data trustworthiness is also an area where extensive research is needed. This study is an attempt to demonstrate the practical implementation of a simple cryptographic algorithm for data encryption and decryption on a hardware and software-based platform.

Literature Review

Data security is indispensable in all sectors of our day-to-day lives such as the healthcare, financial, educational sectors etcetera. Educators, students, other stakeholders and the relevant professionals have a key role to play in ensuring that an ethical, responsible and civic-conscious education in the usage of new data-centered technological innovations is a priority for action, especially in this digital era. This can be achieved through the provision of risk awareness, development of critical-thinking skills in using private data, acquisition of relevant knowledge, competencies and familiarity with digital rights and policies, adoption of teaching methodologies that helps people in navigating the digital world confidently and lucidly and being respectful of everyone's right. These are very important steps in the dissemination and promotion of the security of private/personal data in each sector such as the educational sector [8-9].

The fundamental guiding principles are based on the knowledge and understanding of what constitute a private data, the need for personal data security, the respect for the privacy of others and an understanding of the digital world in terms of the technical infrastructure, hardware, applications and software of information architecture supporting the deployment of data-centric technologies. A basic knowledge about pseudonymity and the masking of a user's identity and the notion of metadata are equally important. Each party involved should gain familiarity with the usage of technical devices for identification, authentication, authorizations, secured collection of private data and data encryption and decryption solutions. This is mainly due to the fact that secure and reliable data storage and sharing is achievable through the use of effective data encryption and decryption approaches [5-6].

Current approaches employed in securing data involve biometric technologies and cryptography. From time immemorial, cryptographic algorithms have been adopted as very important tools for data security and the prevention of unauthorized access to personal, private or confidential data. The cryptographic authentication process relies heavily on the possession of the encryption and decryption keys [9].Data encryption is the process of employing a particular computational or mathematical algorithmic framework to transform a plaintext into an un-

intelligible text referred to as the ciphertext. The reverse operation to encryption is the data decryption process that involves the transformation of the ciphertext back to the original plaintext. These processes allow the secure transmission, storage and sharing of confidential data over an unreliable medium such as the Internet [10].

Several research studies have investigated the use of cryptosystems in securing confidential information. Jagadeesanet al.[11]proposed a method using a protected cryptographic key generated from multimodal biometrics. The work further improved security based on the difficulty associated with the factorization of large numbers and a multiple biometric template was employed to create a 256 bit cryptographic key. In a similar manner, Abuguba et al. [12] proposed a cryptographic key creation from biometrical features based on trait fusion at the feature level and the biometric template construction using filtering and the principal component analysis. The generated template is then employed to create a very efficient 256 bit cryptographic key for data encryption.

The authors in [13] proposed a data encryption algorithm based on the theory of chaotic diffusion. The initial data encrypted through chaotic diffusions is transferred via a wavelet transformation for converting the signal to the frequency domain. An inverse wavelet transform is then employed for transformation from the frequency domain back to the original data. The algorithm guarantees the integrity as well as the privacy of the transmitted or stored data. The author in [14] provided a data encryption algorithm based on the chaos theory in which the data is divided into multiple color planes such as Blue, Green and Red planes. The chaos theory is then applied separately on each of the color planes. Subsequently, the individually encrypted color planes are then integrated to form the ultimate encrypted data. The studies are all theoretical in nature; this study therefore provides a realistic implementation of cryptographic algorithm using commercially available FPGA board and the Verilog software platform as a demonstration of such implementation.

Application: Implementation of a Data Encryption and Decryption Algorithm

The complexity of mathematical concepts such as discrete logarithmic problem (DLP) and the integer factoring problems are the basis for the security of modern public-key crypto-graphical systems. However, it is a known fact that each digital signature and key exchange mechanism being used today is at risk of being broken with a quantum computer except for the sub-division of cryptosystems called post-quantum cryptosystem (PQC) [8]. Current research efforts have focused on theoretical abstractions based on four main classes of cryptosystems: code-based cryptosystem, hash-based cryptosystem, multivariate cryptography and lattice-based cryptosystem. The differences among the four frameworks depend on the complexity of the foundational mathematical problem, the length of the ciphertexts, key lengths and the performance. To go a step further than the theoretical studies, this work provides a software and hardware-based implementation of a simple crypto-graphical algorithm.

Based on the type of keys used, cryptosystems algorithms are categorized into symmetric-key and asymmetric-key cryptosystems. In the symmetric-key systems, a single key is used by both the sender and the receiver while the symmetric-key systems employ two different keys: the first is a public key that is known to all the parties involved and the second is a private key that is only disclosed to the authorized receiver of the data. This is done to increase the difficulty for an adversary to gain access or guess the key values and have the ability to compromise the data or corrupt the integrity and trustworthiness of the information.

This section aims to introduce the design and implementation of a data decryption and encryption algorithmic module using NEXYS 2 board and Xilinx ISE 14.6 development tool kit. The designed and implemented system encrypts and decrypts all alphanumeric characters. The system will be very vital in situations where privacy, confidentiality, integrity and secrecy of data

transmission are of paramount importance. The design is also appropriate for Field Programmable Gate Array (FPGA) Implementation. This design is applicable in instances where two or more partiesexchange private and confidential information without the possibility of eavesdropping nor attack from a malicious adversary. For example, transactions involving the transmission of sensitive information over an unsecured medium may be compromised without a strong encryption and decryption algorithm in place.

The typical system to be implemented takes in alphanumeric inputs called plaintexts and generates an encrypted alphanumeric output called the ciphertext. The designed cipher is a modified substitution cipher based on the substitution algorithm. It simply takes in binary inputs equivalents of the inputs and substitutes them with a different letter/number at the output based on a unique key (symmetric key). The decryption system must use the exact key to decipher the ciphertext and recover the original plaintext input. The key used is made dynamic so that a key is never used twice to make it difficult for the adversary to guess the key values.

As a conceptual introduction to the plaintext-ciphertext mapping, Figure 1 shows an example with a key, K=4. Here, the ciphertext is obtained by substituting each character in the plaintext with its equivalent character based on the key value. The ciphertext value is read off directly from the table based on the key values and the plaintext entries. This is one example that introduces the concept of plaintext to ciphertext mapping in a classical encryption algorithm.

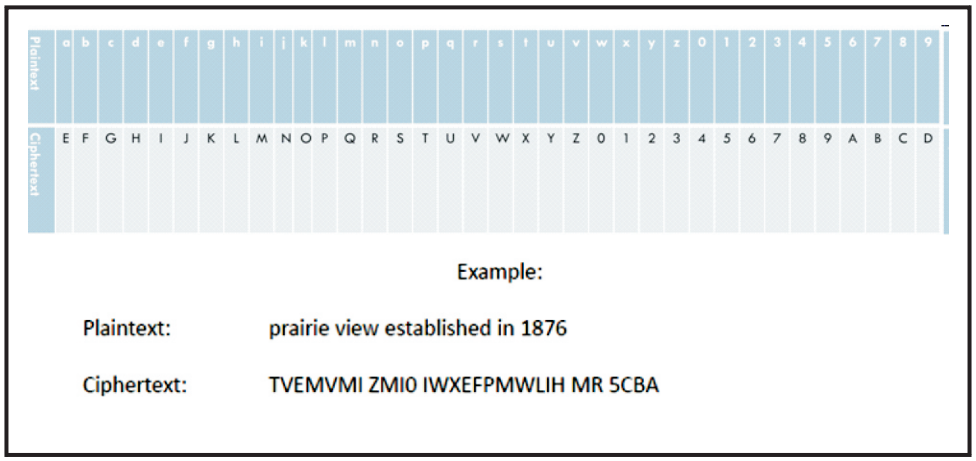


Figure 1: A conceptual plaintext-ciphertext mapping.

The implementation phase relies on an encryption and decryption truth table similar to the one shown in Table I and Table II respectively where the alphanumeric plaintext and ciphertexts are converted to their binary equivalent for implementation on an FPGA.

Table I: A conceptual data encryption truth table.

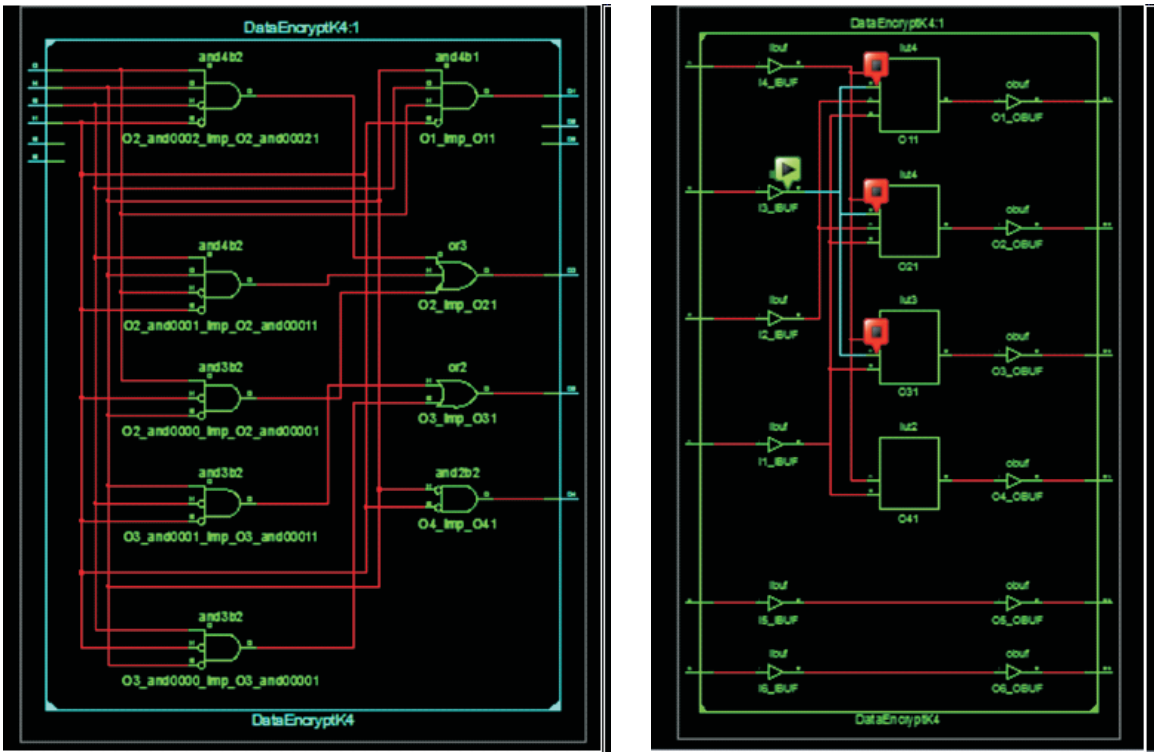
Input Plaintext	Binary Equivalent Of Input Plaintext		Binary Equivalent Of Output Ciphertext	Output Ciphertext
	$I_1 I_2 I_3 I_4 I_5 I_6$		$O_1 O_2 O_3 O_4 O_5 O_6$	
0	000000		000100	4
1	000001		000101	5
2	000010		000110	6
3	000011		000111	7
a	001010		001110	E
b	001011		001111	F
c	001100		010000	G
d	001101		010001	H

Table II: A conceptual data decryption truth table

Input Plaintext	Binary Equivalent Of Input Plaintext		Binary Equivalent Of Output Ciphertext	Output Ciphertext
	$O_1 O_2 O_3 O_4 O_5 O_6$		$I_1 I_2 I_3 I_4 I_5 I_6$	
4	000100		000000	0
5	000101		000001	1
6	000110		000010	2
7	000111		000011	3
A	001010		000110	6
B	001011		000111	7
C	001100		001000	8
D	001101		001001	9

This is to ensure that the data stored, shared or transmitted is not in a plaintext format but rather in an undecipherable or unintelligible ciphertext format for system security enhancement. The mapping from plaintext to ciphertext may go through multiple rounds of reiterations and transformations to make it even more difficult to decipher or decode the plaintext information contained in the data. Then the decryption system uses an identical reverse set of rounds of reiterations and transformations similar to the ones at the encryption end to recover the original data using the same key used to encrypt the original plaintext data.

The synthesis of the design was performed using the Xilinx ISE 14.6 development tool kit and the design synthesis was successful. The RTL and technology schematics are shown in Figure 2. Figure 2(A) shows the encryption RTL schematics while Figure 2(B) depicts the encryption technology schematics in a typical FPGA implementation using the Verilog software.



(A) (B)

Figure 2: Encryption and decryption implementation. (A) Encryption RTL Schematics (B) Encryption Technology Schematics

Most design fail as a result of inconsistent timing scheduling. Thus it is important to account for timing verification. The design timing is limited by the speed of the logic cells on the Spartan 3E FPGA on the NEXYS 2 board. The design is simulated using the ISE simulator (ISim) software embedded in the Xilinx ISE 14.6. It exhausts all possible inputs and the timing waveform was exactly as expected. Figure 2 shows the waveform for the data encryption module. A reverse but identical implementation step is carried out for the data decryption module as well.

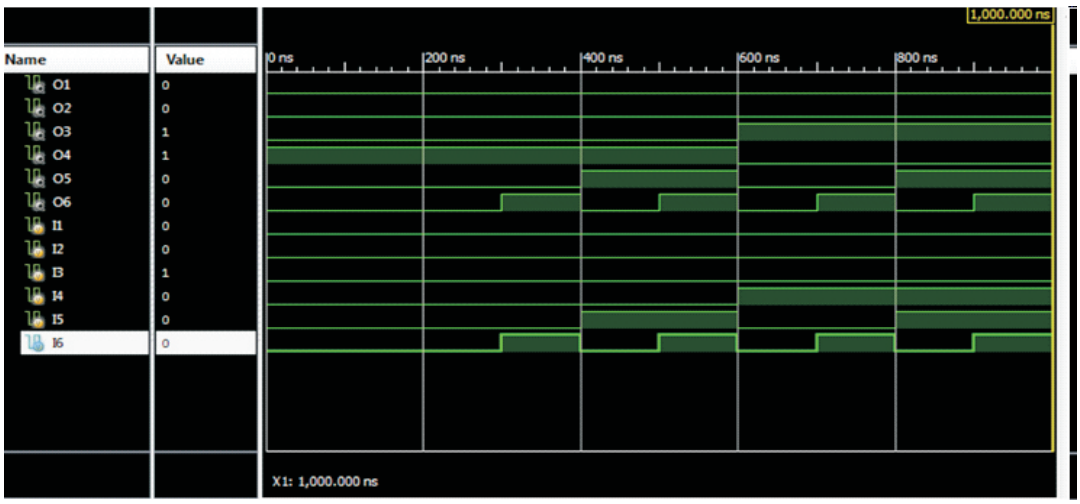


Figure 3: Waveform for the data encoder

The timing verification of the design is very critical. When the encryption and decryption codes are executed on the board, the input and output data correspond to the NEXYS 2 boards LED lights.

Concluding Remarks

Unfortunately, the solutions offered by several data security and privacy protection corporations are too complicated and cumbersome to use for most clients, administrators and stakeholders. A six-year-oldchild may know how to make a call or watch a video on a mobile phone, but can he or she figure out the usage of security software? One of the main issues for a data security company is the creation of a solution that can be integrated seamlessly into everyday lives. Thus data security and privacy protection must be, if possible, simple, ubiquitous, and easily understood by the relevant entities. This will help in preserving one of the most impactful inventions of the last century and help our world to continually prosper, develop and innovate.

Thus, this study focuses on the design and implementation of a simple and easy data decryption and encryption algorithmic module using the field programmable gate array (FPGA) NEXYS 2 board and Xilinx Integrated Synthesis Environment (ISE) 14.6 development tool kit.The choice of which cryptographic algorithm to be used is dependent on factors or requirements such as security needs, specific application, processing resources, cost, speed requirement and capability of design. Individuals or large entities can secure private data and information through an understanding of encryption and decryption mechanisms. Although it is highly unethical, day-to-day communications between/among individuals are monitored constantly. Those monitoring the communication may include identity thieves, hackers, Internet service providers, governments etcetera. By learning the usage of cryptographic encryptions for secure communications, one can safeguard one's data from compromise.

REFERENCES

[1] Bertino, E. 'Introduction to Data Security and Privacy', Journal of Data Science Engineering, Vol 1, pp125–126, September 2016.

[2] K. Hamsha and Nagaraja G.S, 'Analysis of Security Mechanism Using Threshold Cryptography for Hierarchical Wireless Sensor Networks', International Conference on Communication and Signal Processing, pp 1938-1941, India, April 2017.

[3] Bertino, E., 'Big data—security and privacy'. 2015 IEEE international congress on big data, New York City, NY, USA, June 2015

[4] Bertino, E. 'Data trustworthiness—approaches and research challenges. Data privacy management, autonomous spontaneous security, and security assurance' 9th international workshop, DPM 2014, 7th international workshop, SETOP 2014, and 3rd international workshop, QASA 2014, Wroclaw, Poland, September 2014.

[5] Bertino, E. 'Data security—challenges and research opportunities. Secure data management', Proceedings of 10th VLDB workshop, SDM 2013, Trento, Italy, August 2013.

[6] Yi, X. et al, 'Homomorphic encryptions and application'. Springer briefs in computer science. Springer, pp 1–126, 2014.

[7] Rezvani, M. et al, 'Secure data aggregation techniques for wireless sensor network in the presence of collusion attack'. IEEE Transaction on Dependable Secure Computing 12(1):98–110, 2015.

[8] C. Cheng et al., "Securing the Internet of Things in a Quantum World," IEEE Communication Magazine, vol. 55, no. 2, Feb. 2017, pp. 116–20.

[9] K.O. Oluwadamilolaet al 'An Improved Authentication System Using Hybrid of Biometrics and Cryptography', proceedings of 2017 IEEE 3rd International Conference on Electro-Technology for National Development, pp 457-463, November 2017.

[10] P. Selvarani and P. Visu, "Multi-model Biocryptographic Authentication in Cloud Storage Sharing for Higher Security," Res. J. Appl. Sci. Eng. Technol., vol. 11, no. 1, pp. 95–101, 2015.

[11] A. Jagadeesan, et al, "Cryptographic-Key Generationfrom Multiple Biometric Modalities: Fusing Minutiae with Iris Feature," Intl' J. Computing Appl.,vol. 2, no. 6, pp. 16–26, 2010.

[12] S. Abugubaet al"An Efficient Approach to Generating Cryptographic-Keys from Face and IrisBiometrics Fused at the Feature Level," Intl'. J. Computing. Sci. Net.Secur., vol. 15, no. 6,pp. 6–11, 2015.

[13] M. Mishra, S.Pandit, "Image Encryption Technique Based on Chaotic System and Hash Function", 2014 IEEE International Conference on Computer Communication and Systems(ICCCS '14), Feb 20-21, 2014, Chennai, INDIA, 2014

[14] N. Debbarma, L. Kumari, J. L. Raheja, "2D Chaos Based Color Image Encryption Using Pseudorandom Key Generation", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol. 2, Issue 4, July 2013.